# ネットワーク/セキュリティエンジニア
# 知識最低条件

本講習を受講する前での前提知識として、
・ITエンジニアの全体像
・IPアドレス、サブネット、ネットワークについて知識があること
・Level1,2を完全に理解していること

本講習では、
・ネットワークの設計、構築
・セキュリティの設計、構築
をメインとしています。

# ネットワーク/セキュリティエンジニア
# 1．OSI 7階層参照モデル

ネットワークをきちんと階層化して定義したものに、OSI参照モデル（Open Systems Interconnection reference model）があります。これは、表に示すように7階層に定義されています。各階層は、次に示すような機能を規定しています。

| | |
|---|---|
| アプリケーション層 | アプリケーション間のやり取り |
| プレゼンテーション層 | データの表現形式 |
| セッション層 | 接続の手順 |
| トランスポート層 | データ通信の制御 |
| ネットワーク層 | インターネットワークでの通信 |
| データリンク層 | 同一ネットワーク上での通信 |
| 物理層 | ケーブルや電気信号やコネクタなど |

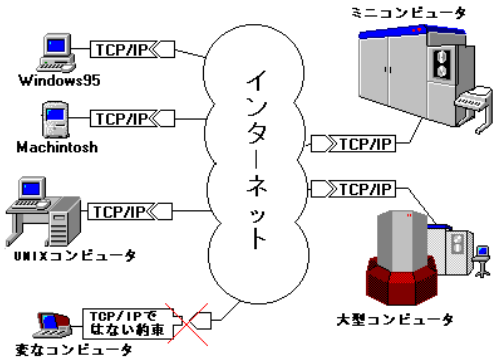
<table>
<tr><th>OSI参照モデル</th><th>TCP/IPの階層モデル</th><th>TCP/IPプロトコル</th><th>コンピュータ上の処理</th></tr>
<tr><td>アプリケーション層</td><td rowspan="3">アプリケーション層</td><td rowspan="3">HTTP, SMTP, POP3<br>FTP, SSH, RIP, SNMP…</td><td rowspan="3">通信アプリケーション<br>プログラム</td></tr>
<tr><td>プレゼンテーション層</td></tr>
<tr><td>セッション層</td></tr>
<tr><td>トランスポート層</td><td>トランスポート層</td><td>TCP, UDP</td><td rowspan="2">OS</td></tr>
<tr><td>ネットワーク層</td><td>インターネット層</td><td>IP, ARP, ICMP, OSPF…</td></tr>
<tr><td>データリンク層</td><td rowspan="2">ネットワーク<br>インターフェース層</td><td rowspan="2">Ethernet, PPP…</td><td rowspan="2">デバイスドライバ<br>NIC</td></tr>
<tr><td>物理層</td></tr>
</table>

コンピュータネットワークやインターネットを動かしている通信技術を一式として総称したものを「TCP/IP」という。
TCPとIPだけではなく、ICMPとかTCPとかHTTPとか色々ある。
とにかくネットワーク越しに何かを送るときに必要なプロトコルだと思えば良い。

# ネットワーク/セキュリティエンジニア
# 2．TCP/IPとは

コンピュータネットワークやインターネットを動かしている通信技術を一式として総称したものを「TCP/IP」という。
TCPとIPだけではなく、ICMPとかTCPとかHTTPとか色々ある。
とにかくネットワーク越しに何かを送るときに必要なプロトコルだと思えば良い。

**現在のインターネット/ネットワーク技術は全て**
**TCP/IPプロトコルである！**




## プロトコルとは？

プロトコルとは「通信規約」のことである。
**•はじめはこのデータ**
**•次はこのデータ**
**•その次はこのデータ**


という風にデータが送られてくる順番を決めておかないと、いったい何が送られて来たのかわからなくなる。
例えば、「宛先」「どこから来たか（自分の住所）」「データ中身」という順番でデータが送られてくるとわかっていたら、受け取った側も「宛先」「どこから来たか（自分の住所）」「データ中身」だと知っていればデータを判別できるわけだ。
だからこそ、プロトコルが必要になる。
**正直ここまで押さえておけば十分である。**
**初心者の方であれば簡単に理解すれば問題ないし、この知識が詳細に必要なのは「パケット解析」など一部の専門職である。**

こうやってネットワークのデータは流れていて、このデータ順序、分別に統一で定義されたものが「TCP/IP」である。
だからTCP/IP以外で通信するものはほとんど無いし、あったとしてもTCP/IPにしなければ通信できないのである。

# ネットワーク/セキュリティエンジニア
# ３．OSI7階層によるネットワーク機器

| | |
|---|---|
| アプリケーション層 | アプリケーション間のやり取り |
| プレゼンテーション層 | データの表現形式 |
| セッション層 | 接続の手順 |
| トランスポート層 | データ通信の制御 |
| ネットワーク層 | インターネットワークでの通信 |
| データリンク層 | 同一ネットワーク上での通信 |
| 物理層 | ケーブルや電気信号やコネクタなど |

## Cisco製品

Catalyst3750

L3スイッチ

Catalyst2960

L2スイッチ

## その他製品

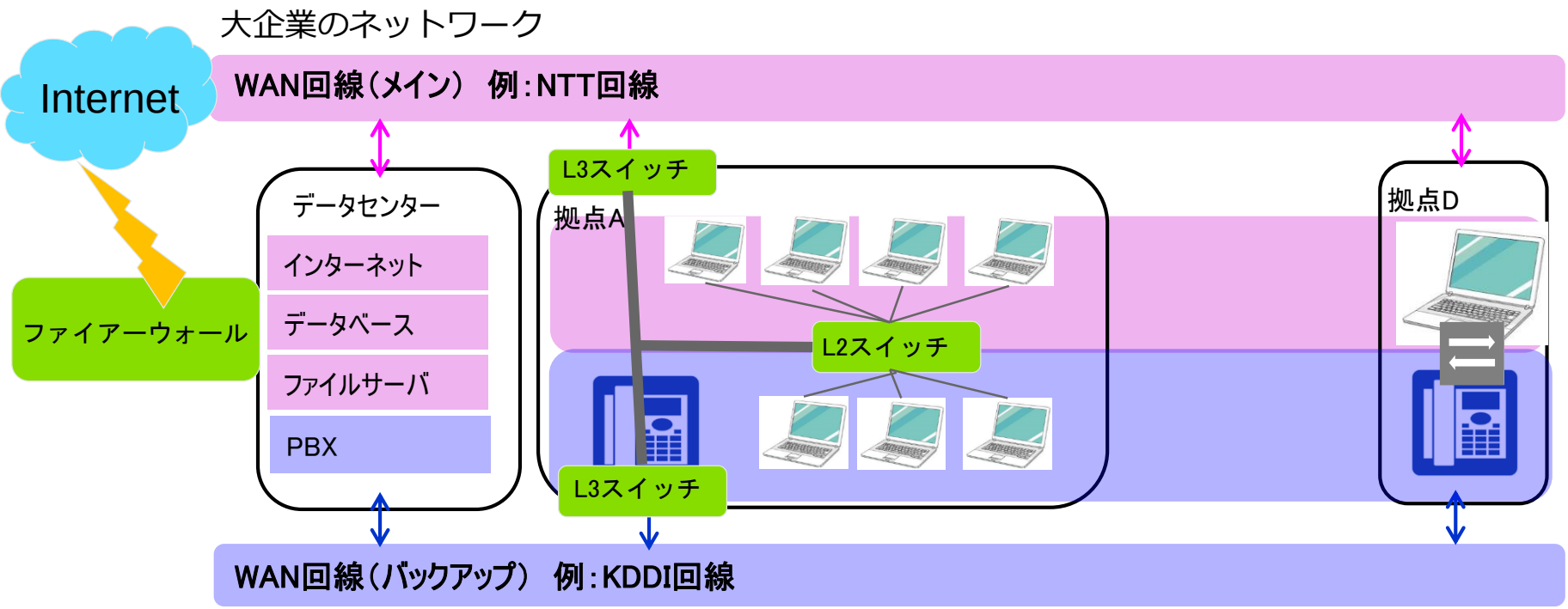
F5社

WAF

Juniper社　Palo Alto社

ファイアーウォール

# ネットワーク/セキュリティエンジニア
# ４．LANとWAN,スイッチとファイアーウォール




簡単に説明すると、L2スイッチはハブ。L3スイッチはネットワークを分ける機器。
ファイアーウォールはインターネットとの境界線、ゲートウェイ。
いわゆるセキュリティ機器というのはL2スイッチとL3スイッチは含まず、ファイアーウォールなど
ゲートウェイにある機器を指す。

# ネットワーク/セキュリティエンジニア
# ５．なぜ機器が決まっているのか

大企業のネットワークはデータのやり取りが膨大な量となり、スーパースペックを誇る処理能力が必要。

昨今ではさらにデータ量が膨大になり、複雑なパケット（データ）も増えてきた（IP電話など）

スーパースペックを誇るL2スイッチ、L3スイッチは、Cisco社しかない！！

大企業のネットワークはデータのやり取りが膨大な量となり、スーパースペックを誇る処理能力が必要。

昨今ではセキュリティ強化、情報漏えい対策、外部からの攻撃対策で
パケットの中身解析が必要になってきた。

セキュリティ対策の詳細は外部には明かせない（明かしたらその上を行く攻撃者が現れる）

だからセキュリティ対策に実績のある、イスラエル製「Palo Alto」や「Juniper」などが選ばれる。

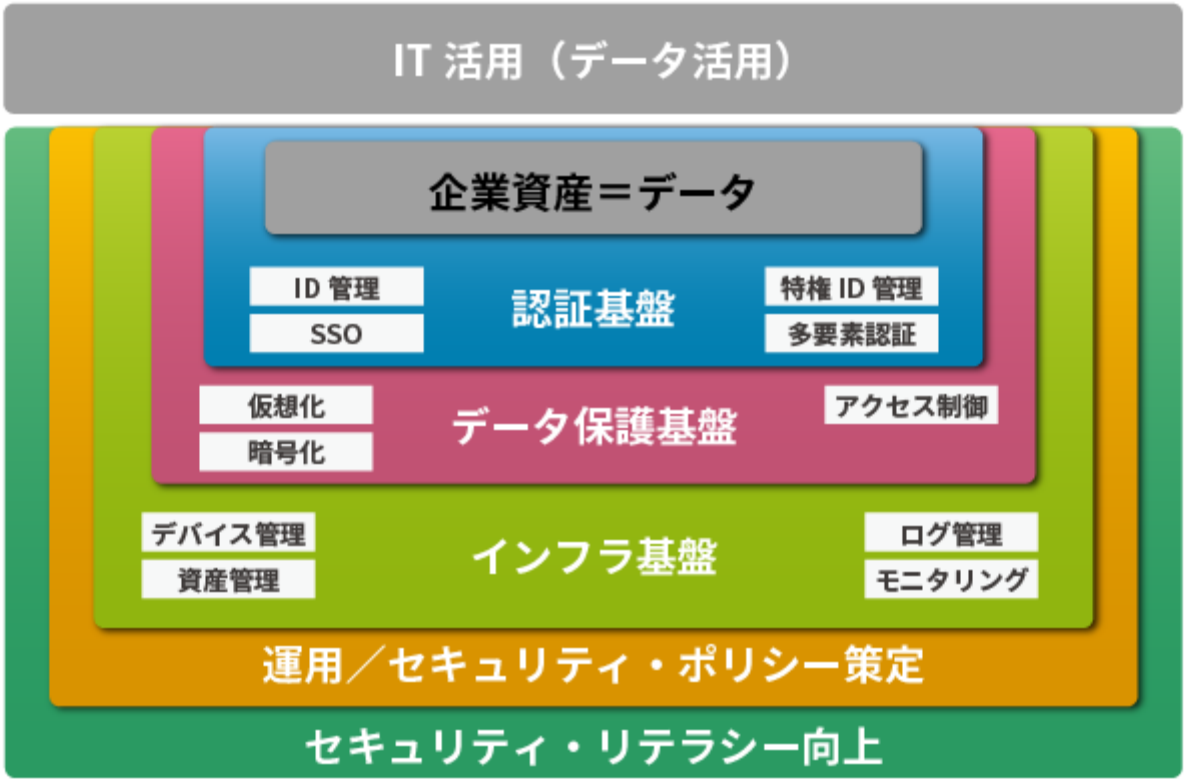
# ネットワーク/セキュリティエンジニア
# ６．具体的なセキュリティ対策

## セキュリティ対策（外部からの攻撃）


セキュリティ対策に100%は存在しない！
重複してセキュリティ対策を行うので、セキュリティ需要は高い！

# ネットワーク/セキュリティエンジニア
# 7．具体的なセキュリティ対策

セキュリティ対策（内部から攻撃）




セキュリティ対策に100%は存在しない！
重複してセキュリティ対策を行うので、セキュリティ需要は高い！

# ネットワーク/セキュリティエンジニア
# 7．セキュリティはインフラ・アプリ・DBの複合

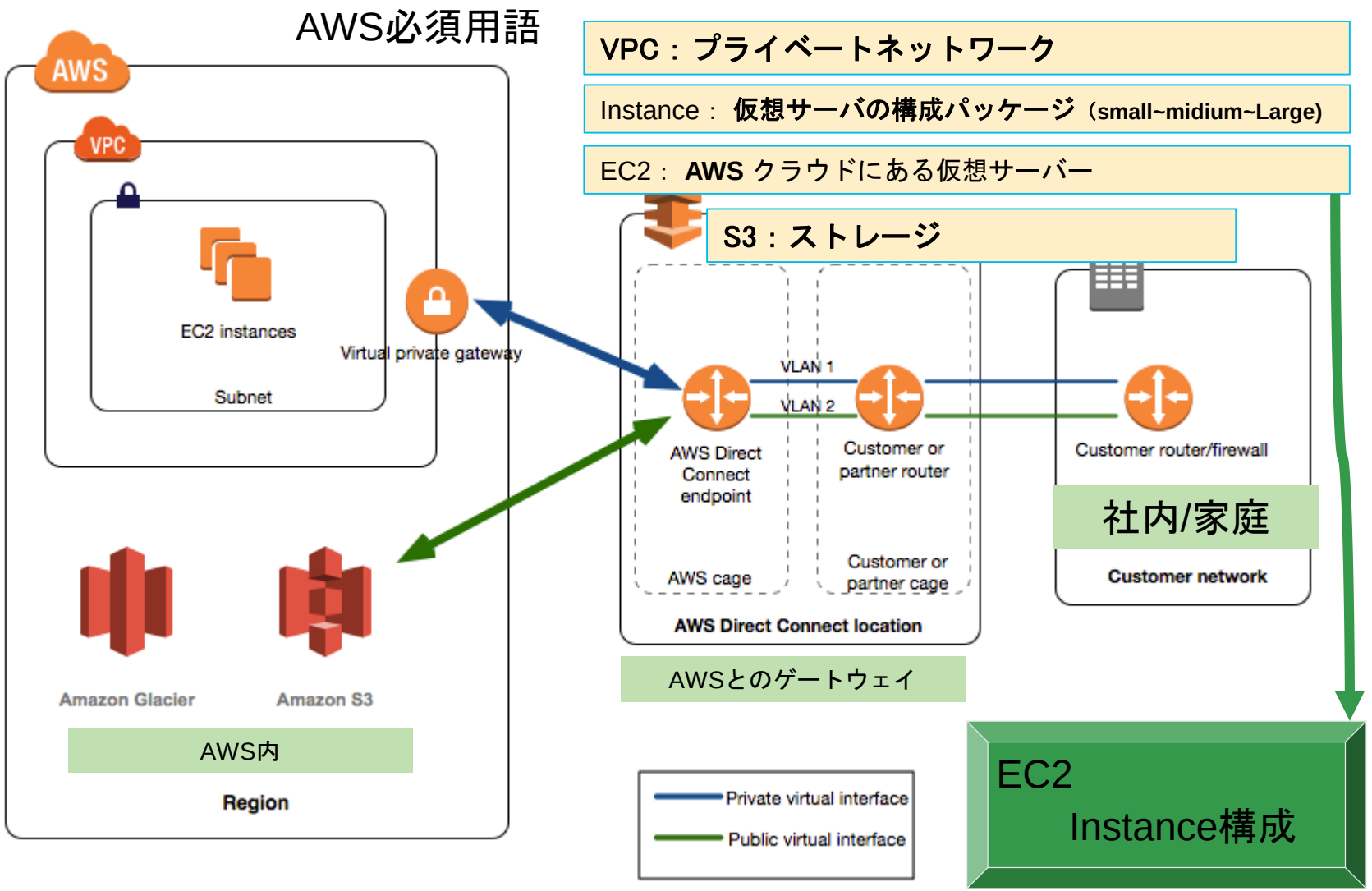
CIO（セキュリティ対策決定）

総合的管轄（マネージャ）

インフラ対策　　アプリ対策　　DB対策

| | |
|---|---|
| PC対策 | Windows Updata / ログ記録ソフト |
| NW対策 | ファイアーウォール /PROXY/通信ログ収集 |
| サーバ対策 | 各種セキュリティログの保存、ファイルへのアクセス記録 |

# ネットワーク/セキュリティエンジニア
# 8．AWSなどのクラウドでの構築



# ネットワーク/セキュリティエンジニア
# ９．クラウド種類

他にはMicrosoftのクラウド（Azure）が有名だが、AWSの1択となっている。

以前はセキュリティなどが不安という声が大きかったが、流れを変えたのは、
米国国防省のサーバがAWSに移行したこと。
世界最高峰のセキュリティを保持する国防省がAWSに移行したことにより、
一気に安全と言う流れとなり、移行が加速した。

いまや**AWS＝世界最高峰のセキュリティ**といわれている。

「管理」「コスト」の部分でもAWSに移行しない理由は無い。

なお、費用面でAzureとAWSはほぼ機能差が無い。

実際にAWSは無料でアカウントを作り構成できるので勉強で試して欲しい！
費用算出も無料でできるので見積もりも作成してみてほしい！

# ネットワーク/セキュリティエンジニア
# １０．実際に実務経験を積む

① Config（設定）を行う

② 基本設計を行う

どちらが重要か？

② 基本設計を行うが重要！

①をどのくらい時間をかけていても全体像が分からず作業者のままである。メーカーによって設定の仕方も異なる。
①は後からでも覚えられる。WEBで調べればすぐ分かる。

例えて言うと、ビルを構築する際に、柱の組み立て方を勉強するのと、ビル全体像を勉強する違い。

中小のSierでは①が重視される。
社内SEや中堅以上では②が重視される。

個々のConfigは調べれば分かるが、基本設計など「上流」をやるのが得意です！
と面接で言えばかなり好印象！！

なぜなら上流が出来る人が圧倒的に少ないから！

# ネットワーク/セキュリティエンジニア
# １１．実際に実務経験を積む（２）

①　Config（設定）を行う　　：　　単価40万/月程度

②　基本設計を行う　　：　　単価70万/月以上

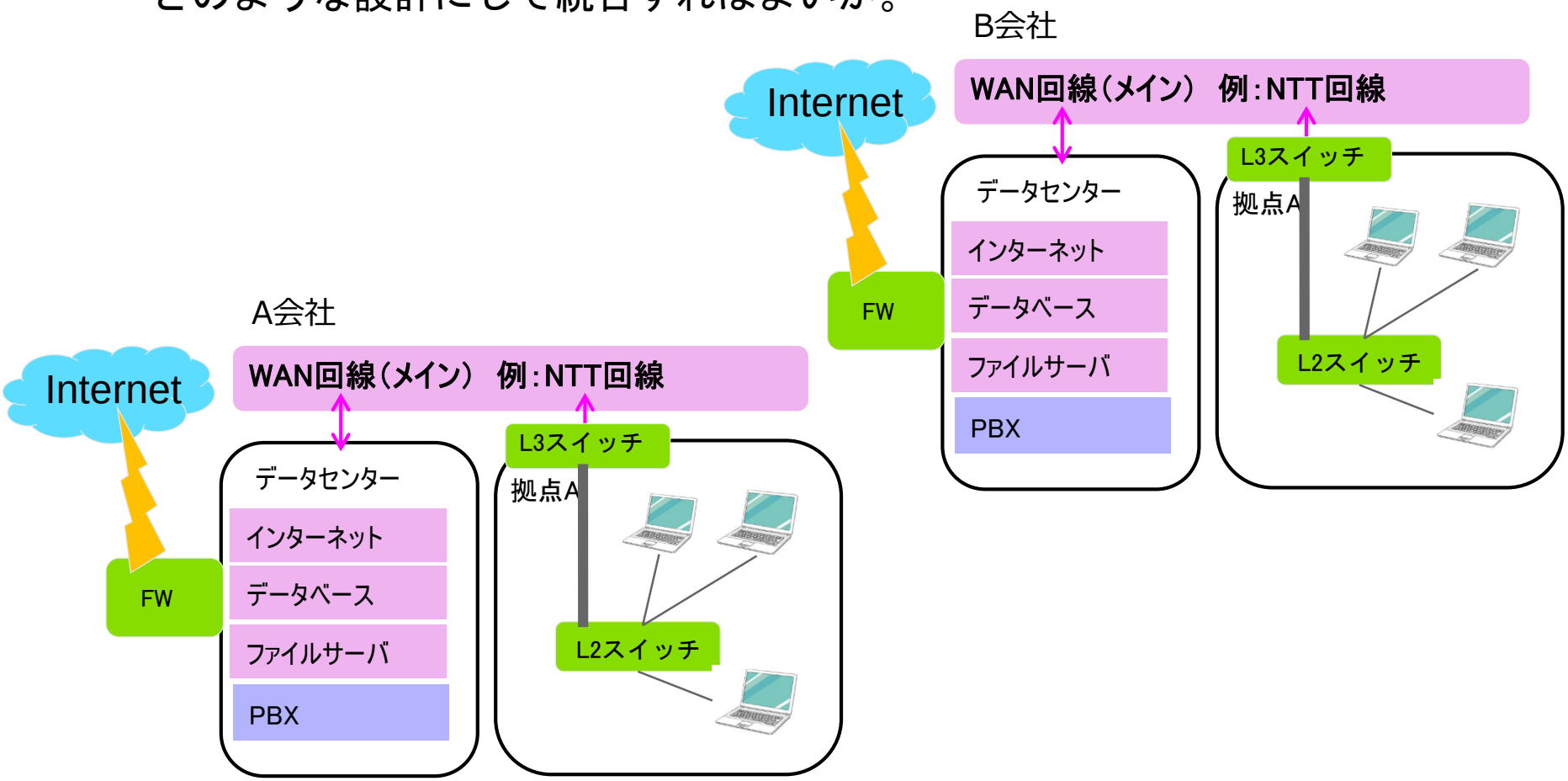
設計をマスターするには、ネットワークの基本を理解して、
実際の顧客の要望を絵にするのが重要！
①しか出来ない人はネットワークの基本を理解していない！！（6割の人がそれ）

基本設計　＝　顧客の要望を絵にする！これができれば終了！

ただしある程度、こういう設定ができる、できないを知っておく必要がある。
これをマスターするにも、とにかく数をこなすこと！障害の対応を実際に行うこと、実際の機器の設定を見ること。

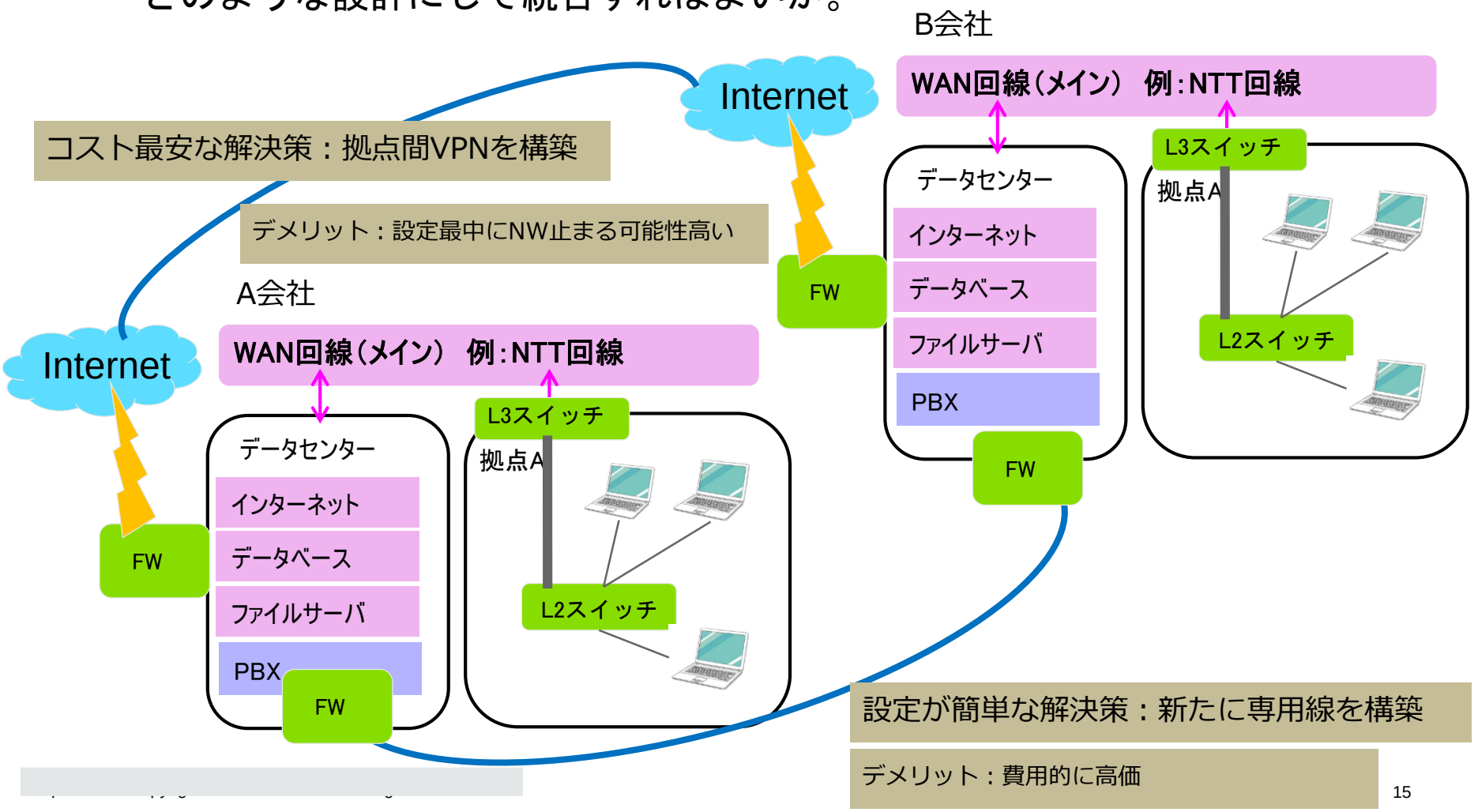
# ネットワーク/セキュリティエンジニア
# １１．実際に実務経験を積む（３）

① A会社とB会社のネットワークを一時的に統合したい。
どのような設計にして統合すればよいか。



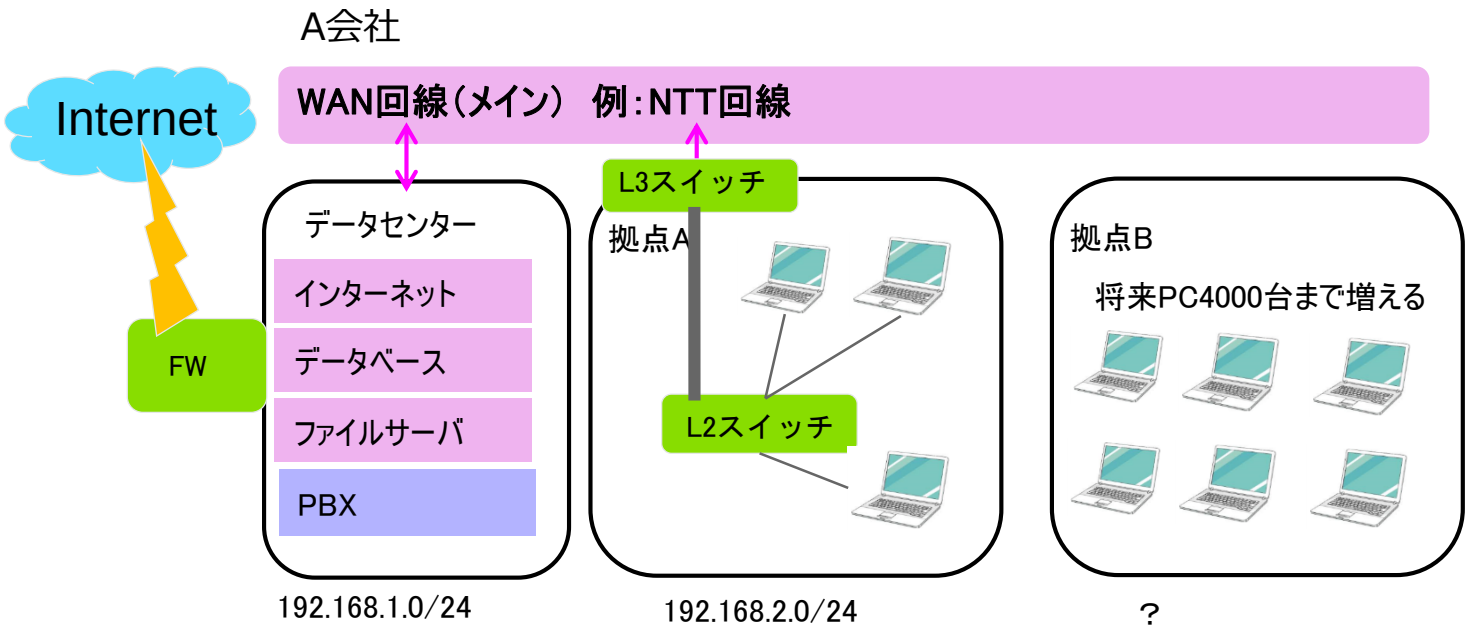
# ネットワーク/セキュリティエンジニア
# １３．実際に実務経験を積む（３）

① A会社とB会社のネットワークを一時的に統合したい。
どのような設計にして統合すればよいか。



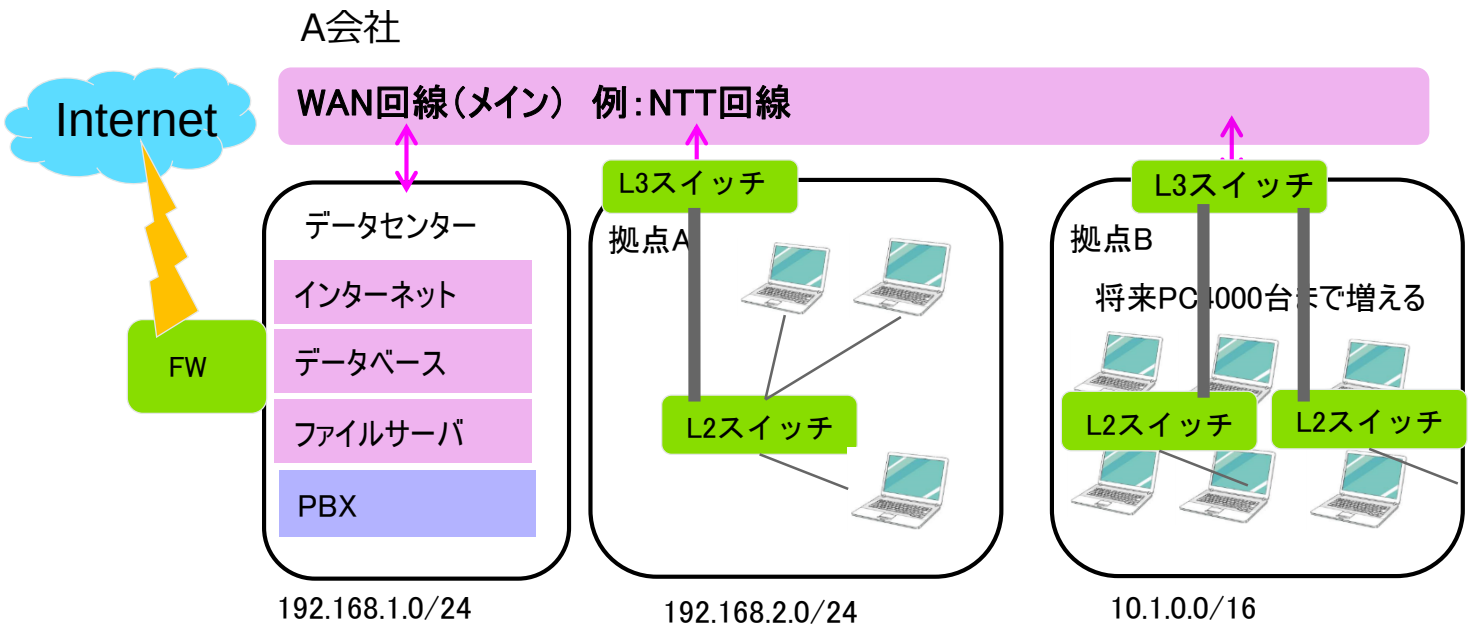
# ネットワーク/セキュリティエンジニア
# １４．実際に実務経験を積む（３）

②　拠点を1つ作りたい、どのようなNW構成にするか、IPアドレスと機器構成を提示して欲しい



# ネットワーク/セキュリティエンジニア
# １５．実際に実務経験を積む（３）

②　拠点を1つ作りたい、どのようなNW構成にするか、IPアドレスと機器構成を提示して欲しい

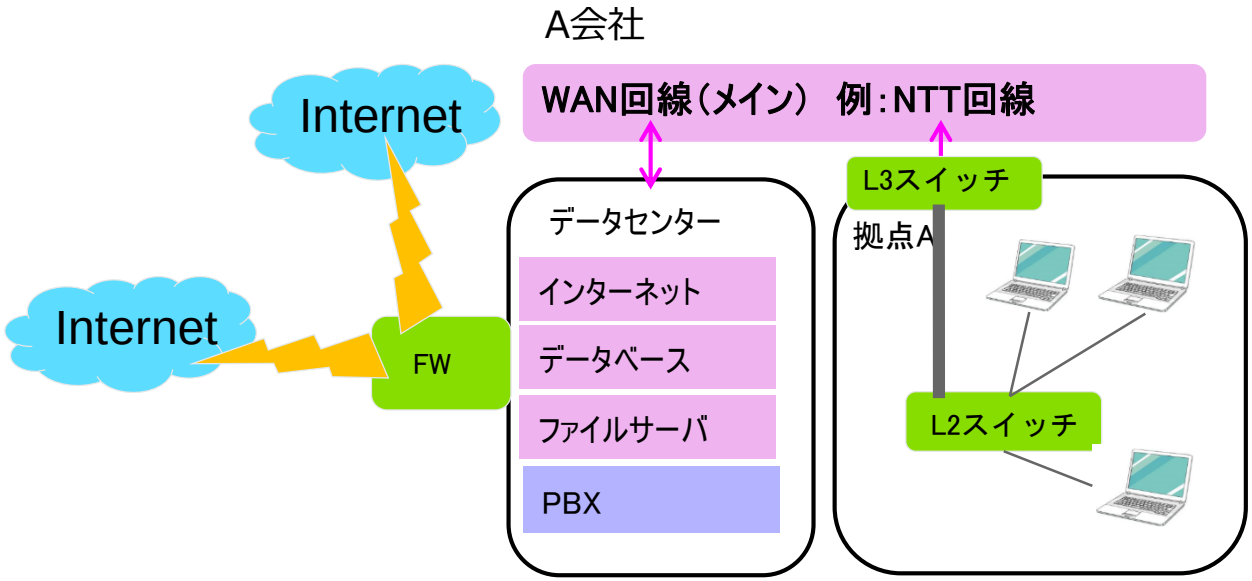



192.168.*.*は/24～/32専用

10.*.*.*は/8～/32まで自由に設定できる

# ネットワーク/セキュリティエンジニア
# １６．実際に実務経験を積む（３）

③　Internetの冗長化（バックアップ）を行いたい、ただしその間ネットワークを長時間止めたくない、どうすればよいか



# ネットワーク/セキュリティエンジニア
# １７．実際に実務経験を積む（３）

③　Internetの冗長化（バックアップ）を行いたい、ただしその間ネットワークを長時間止めたくない、どうすればよいか

(1)まず新しいインターネット回線を引き込む
(2)ファイアーウォールに設定を入れ込む、ただしONにはしない。
(3)テストとして、特定のPC通信のみをバックアップに切り替える設定をONにする
(4)特定PCの通信がバックアップのインターネットに出れることを確認する
(5)全体のPCがメインインターネットが切れたときにバックアップにすぐに移行できるかテストする
（この際は少しの断時間は仕方ない）

作業前に切り戻し手段を手順化しておき、問題発生時はすぐに戻す。

# ネットワーク/セキュリティエンジニア
# １８．難易度

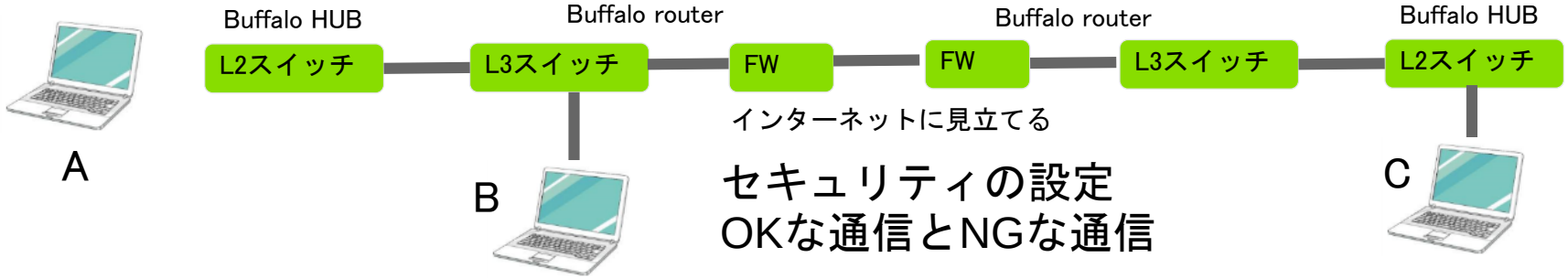
ネットワークエンジニア、セキュリティエンジニアとして最も難しいPJは、
既存のネットワークを新しいネットワークに「切り替え」すること！

新しい拠点追加などは比較的簡単！

切り替えは膨大な手順書と念入りな計画が必要！
ここのPMとして成功できれば、問題なし！

# ネットワーク/セキュリティエンジニア
# １９．実際の機器設定、簡易実務経験

別の日程にて実際に機器を設定する講座を開きます。
方法としては、簡易的なBBルータを複数設定して、ネットワークを構築してもらいます。
これは企業に入っても必ず検証としてやることですので、必須で覚えるべきスキルです。（検証環境構築）
これができるようになれば、大規模になっても問題ないはずです！



# ネットワーク/セキュリティエンジニア
# 実地研修

LANケーブルの種類に注意

LANケーブルはストレートケーブル、クロスケーブルの両方が存在する。

ストレートケーブルはレイヤーが異なる機器の接続、
クロスケーブルはレイヤーが同じ機器の接続に用いる。

一般的に、機器同士の接続はクロスケーブルで接続するポリシーになっている会社が多いので、分別して使い分けよう。

ストレートケーブルとクロスケーブルの見た目の違いは、Google検索などで確認しておこう。

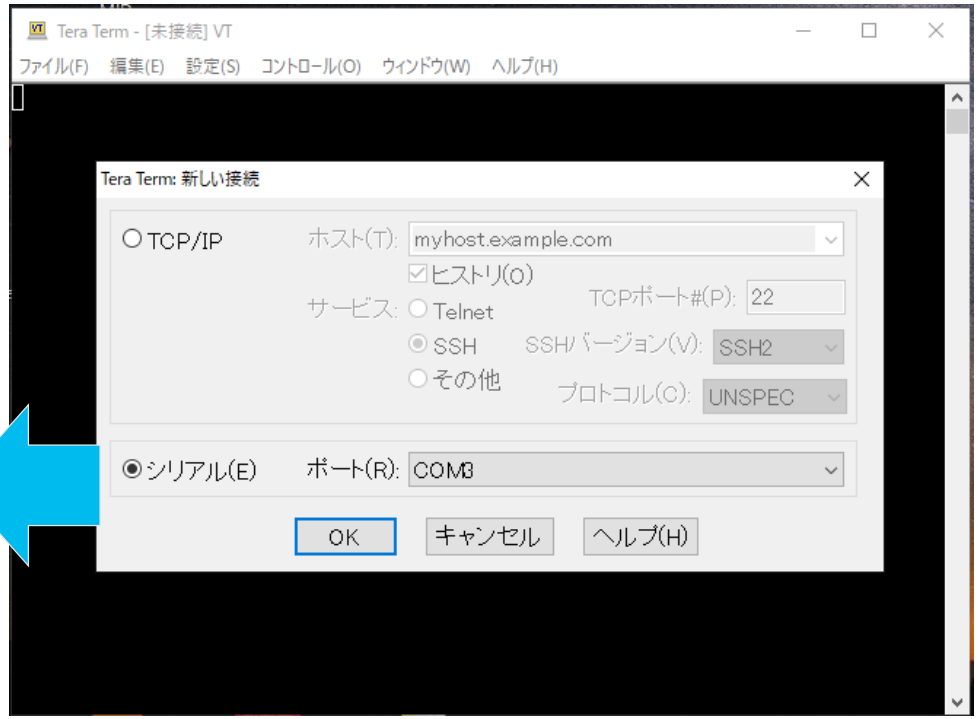
# ネットワーク/セキュリティエンジニア
# 実地研修

Cisco3750（L3スイッチ）　定価２００万　これを使い検証

１．PC設定をしよう
- （１）teraterm のインストール
- （２）コンソールケーブル＋シリアルUSB変換ケーブル用意
- （３）（２）ドライバのインストール
- （４）teratermで機器に接続

機器のConsoleポートに接続する！

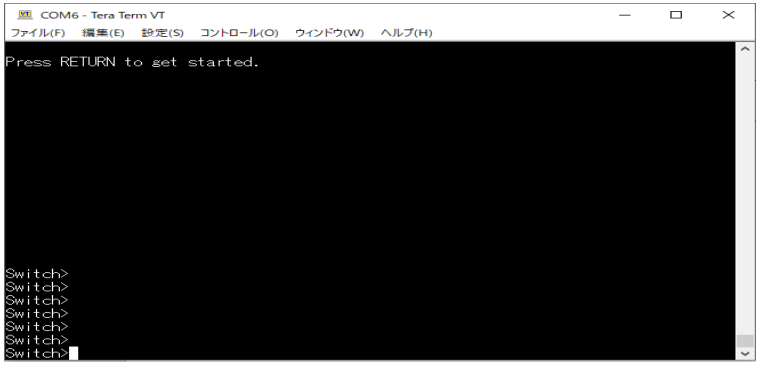
シリアルを選択して、ポートで
USB-XXXと記載のあるものを選択。
無ければドライバが入っていないか、
接続が悪い。

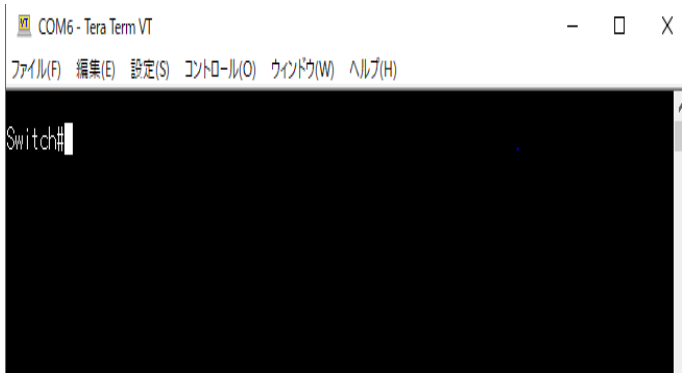
# ネットワーク/セキュリティエンジニア
# 実地研修

## ２．接続しよう

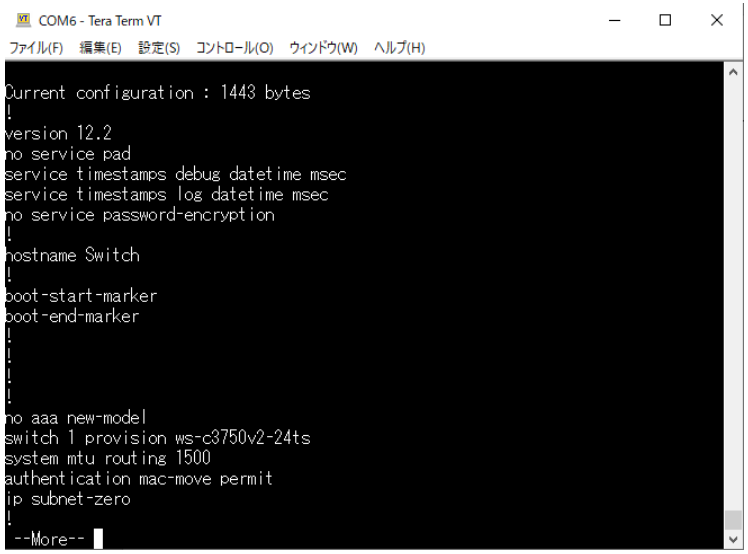
（１）teraterm で機器に接続。Enterを押下して反応を確かめる。

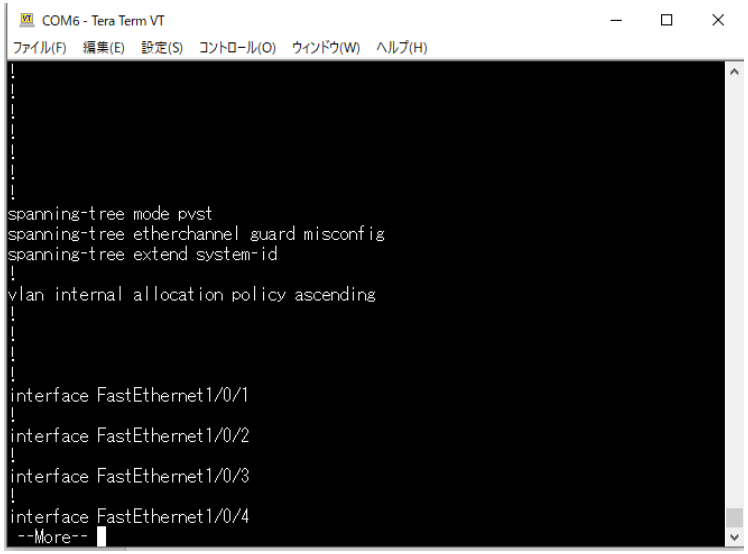



（２）管理者モードに移行します
enと入力し、Enterを押します。
Switch#と表示され、＃が管理者モードを指します。

## （３）設定を確認する。管理者モードでsh run



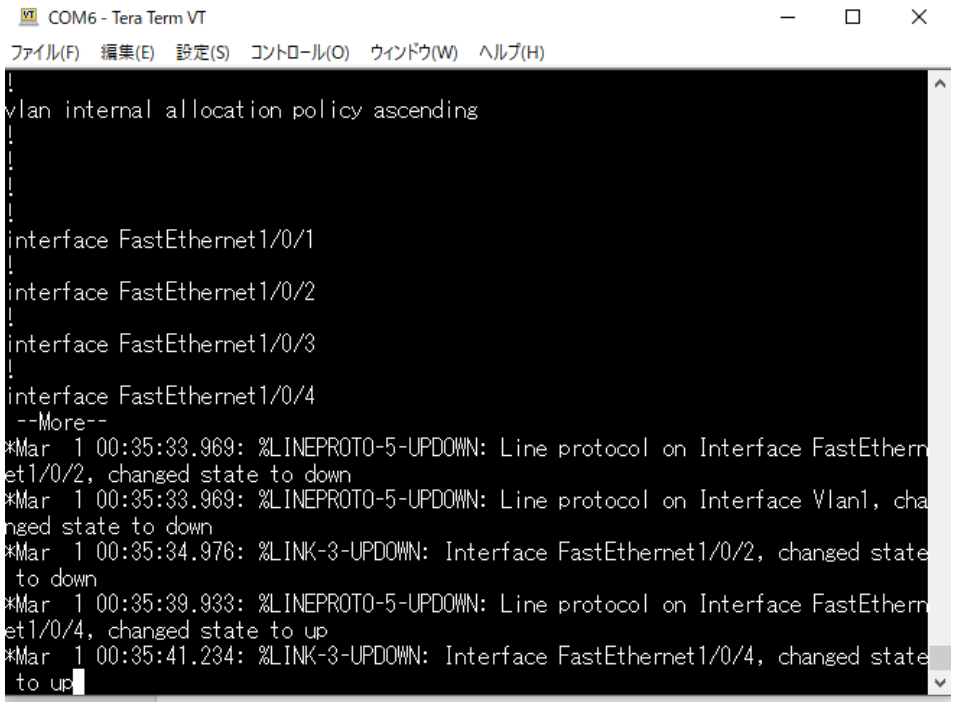

設定内容がすべて表示される。
メモ帳を開きこの内容をすべてコピーすれば、設定のバックアップを取得したことになる。
※パスワード、ユーザなどあらゆる設定が全保存される。
機器を再設定して、貼り付けするときは少しづつ貼り付けしていく。

# ネットワーク/セキュリティエンジニア
# 実地研修

## ３　動作確認する

### （１）各ポートにLANケーブルを接続し、対向側はPCなどに接続する

すると下記のようにリンクアップ警告が表示され、
Interface xxx down、UPと表示され、リンクダウン、アップが検知できる。
これを全ポート実施する。




機器の障害原因のNo1が
インターフェイス障害
であるから念入りに確認。
障害対応でも必須の内容

## ４　設定してみよう

### （１）まず特権管理モード（重要な更新をする最上位Configモード）にする

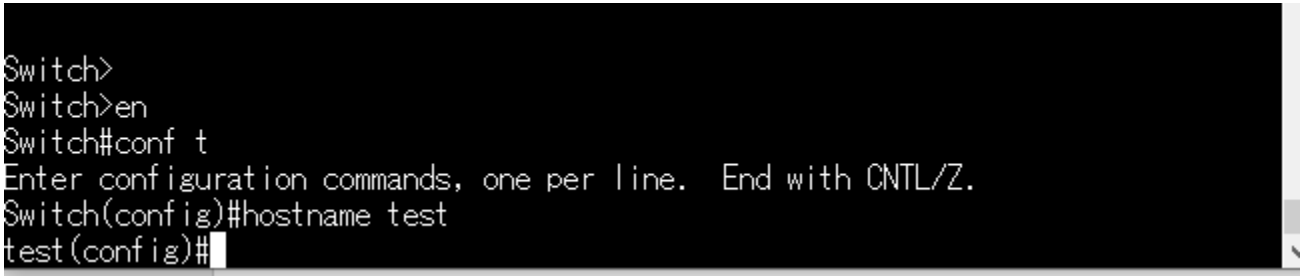
以下コマンドを入力し実行

conf t

### （２）この機器のホスト名を設定する

以下コマンドを入力し実行

hostname test



# ネットワーク/セキュリティエンジニア
# 実地研修

## （３）管理IPアドレスを設定する

test(config)#int vlan 1　　VLAN1のConfigインターフェイスモードへ

test(config-if)#ip address 192.168.1.254 255.255.255.0

```
test#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
test(config)#int vlan 1
test(config-if)#
```

設定完了後Exit２回で抜ける

```
test(config-if)#ip address 192.168.1.254 255.255.255.0
test(config-if)#exit
test(config)#exit
```

設定を保存する。
保存しないと再起動すると設定クリアされてしまう。

test#wr mem

```
test#wr mem
Building configuration...
[OK]
test#
```

（４）設定を確認しよう　　設定が反映されていることを確認できますか？

Sh run

```
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
!
```

```
hostname test
!
```

（５）再起動して設定が保存されていることを確認する

test#reload

System configuration has been modified. Save? [yes/no]: y
Building configuration...
[OK]
Proceed with reload? [confirm]

## （６）複数のVLANを作ろう

```
test(config)#int vlan 2
test(config-if)#ip add
test(config-if)#ip address 192.168.10.254 255.255.255.0
test(config-if)#

test(config-if)#int vlan 3
test(config-if)#ip address 192.168.20.254 255.255.255.0
```

**これでVLAN2、VLAN3が作成された。**

# ネットワーク/セキュリティエンジニア
# 実地研修

## （７）各インターフェイスにVLANを割り振ろう

| | |
|---|---|
| test#conf t | Configモード |
| test(config)#int fa 1/0/1 | Interface 1 に入るモード |
| test(config-if)#switchport access vlan 2 | VLAN2を割り振る、Accessモードで |
| test(config-if)#switchport mode access | Accessモードであることを定義 |
| test#conf t | Configモード |
| test(config)#int fa 1/0/10 | Interface 10 に入るモード |
| test(config-if)#switchport access vlan 3 | VLAN2を割り振る、Accessモードで |
| test(config-if)#switchport mode access | Accessモードであることを定義<br>Accessモードであることを定義 |
| test#wr mem | 設定したら必ず保存 |

# ネットワーク/セキュリティエンジニア
# 実地研修

## （８）設定を確認

test#sh run



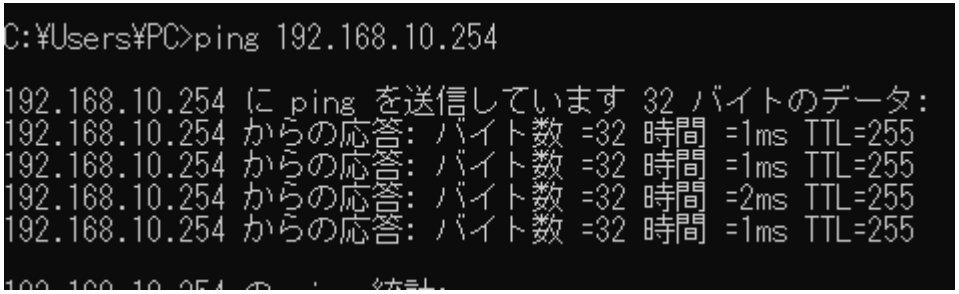
## （９）パソコン側の設定を変更

機器と通信確認をするため、通信ができる設定に変更する

Ipアドレス：192.168.10.5 subnet：255.255.255.0 デフォルトゲートウェイ：192.168.10.254

## （１０）パソコン側からPingで通信確認をする

PCのコマンドプロンプトを開き、Ping 192.168.10.254を実行する




応答が返ってくることがわかる。これで機器とのネットワーク通信（L3レベル）がOKなことを確認できた

この確認方法は基礎中の基礎だから必ず覚えること

```
test#ping 192.168.10.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
test#
```

機器側からPing 192.168.10.5を実行するとPCとの通信ができることがわかる。

この状態でping 192.168.20.254やping 192.168.1.254を実施しても疎通できない。なぜか？
※プロでもはまりやすい。

# ネットワーク/セキュリティエンジニア
# 実地研修

## （１１）テストする通信Interfaceはリンクアップさせる

この場合機器側のVLAN1、3に割り振ったInterfaceがリンクアップしていないため、通信確認ができない。これをテストで行うには強制的にInterfaceをリンクアップさせる。
※以下の方法はテストでしか実施してはいけない！！（ループするため）
Interface10とInterface1と10以外の場所をストレートケーブルで接続する。

これでPing 192.168.20.254と192.168.1.254がPC側から疎通が通ったと思う。
これでPC側からは機器の全VLAN-Interfaceに通信がOKになったことを示す。

コンソールケーブルを外してもOKとなった。

## （１２）機器のパスワード設定

**Console接続パスワード**

test(config)#line console 0
test(config-line)#password "0000"
test(config-line)#login
test(config-line)#exit

**管理者パスワード**

test(config)#enable se
test(config)#enable secret "0000"

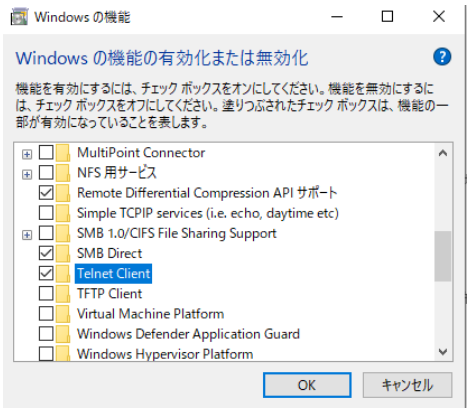
**Te;netパスワード**

test(config)#line vty 0 4
test(config-line)#password "0000"
test(config-line)#login

# ネットワーク/セキュリティエンジニア
# 実地研修

## ５　リモートからのアクセスしてみよう

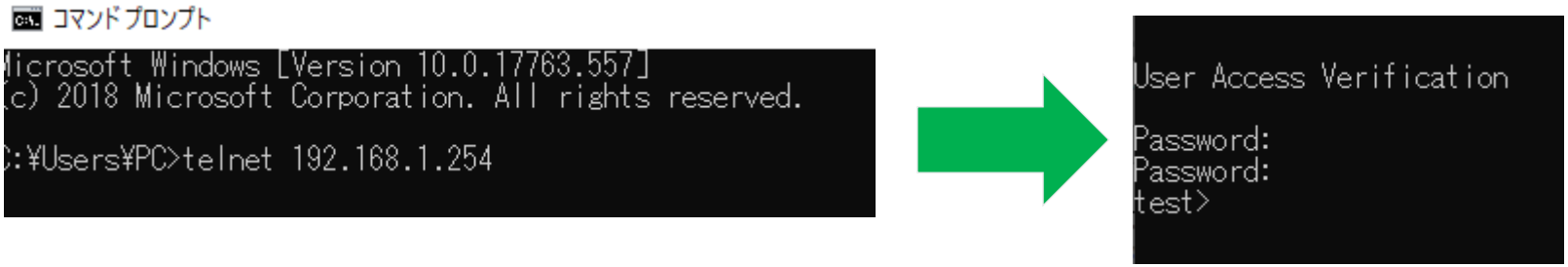
基本的な設定は大体完了です。
この機器を遠隔地に設置したときに、遠隔地から接続できなくてはなりません。
その場合の接続方法は、Telnetです。




Windows7以降はデフォルトで
Telnet機能がオフになっているので、オンにする。

Win10では設定画面でtelnetと検索して、
Telnet ClientをONにする
※詳細は省く

コマンドプロンプトでtelnet 192.168.1.254を実行してパスワード”0000”を入力する　　ログインOK



## ６　L3スイッチの基本的な機能を理解しよう

まずL3スイッチはレイヤー3の機能を搭載しているからレイヤー3の設定が主
（１）VLANインターフェイスとアクセスリスト（ACL）
（２）ルーティング（静的ルーティング、動的ルーティング）
（３）ネットワークの分離
（４）AccessモードとTrunk設定

### （１）VLANインターフェイスとアクセスリスト（ACL）

VLANインターフェイスの設定は以前の項目で済んでいるので省略。
それぞれのネットワーク（VLAN）同士を通信OK、NGに設定するのがACL機能。
ACLはほぼ必ず設定されるものなので、必ず覚えること。

# ネットワーク/セキュリティエンジニア
# 実地研修

札幌拠点にあるL3スイッチにinterface Vlan80,81を作成して、ACLを設定してみよう
ACL名は「Sapporo-CMS-incoming in」

前提条件：既に前項であるVlan1,2,3は作成済みとする

※CiscoのL3スイッチではACL末尾に「In」「Out」表記が必須。文字通りInは入ってくる通信（To）、
Outは出て行く通信（From）であるが、どちらでも同じ機能なので管理上全拠点で統一すべき。
CiscoではIn、Outを末尾で書かなければならない、統一すべき。という点だけ覚えて欲しい。

CiscoのACLにはstandard（標準）とextended（拡張）がある。設定はextendedで行っておけばOK。

```
interface Vlan80
 description Sapporo-KTNET
 ip address 172.18.80.254 255.255.255.0
```

Descriptionというのはコメントのこと。Vlanのコメント。

```
interface Vlan81
 description Sapporo-CMS
 ip address 172.18.89.254 255.255.255.0
 ip access-group Sapporo-CMS-incoming in
```

ACLがない状態で設定すると弾かれるので、下記のACLを設定した後に再度ACLを設定する

```
ip access-list extended Sapporo-CMS-incoming
 10 permit udp any any eq bootps
 20 permit ip any 192.168.0.0 0.0.255.255
 30 permit ip 172.18.89.0 0.0.0.255 host 172.18.80.1
```

ACLの設定手法を覚える。Subnetの逆。Googleで調べる。
192.168.0.0 0.0.255.255 = 192.168.0.0/16を理解する

# ネットワーク/セキュリティエンジニア
# 実地研修

インターフェイスにVLANを割り当てよう

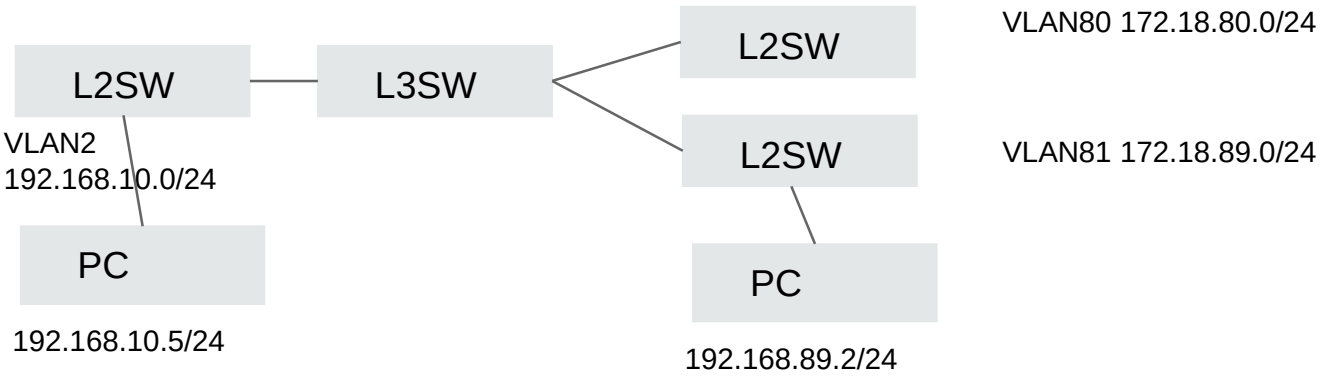
演習：Interface 1/0/11,1/0/12に　→VLAN80を割り当て

演習：Interface 1/0/13,1/0/14に　→VLAN81を割り当て

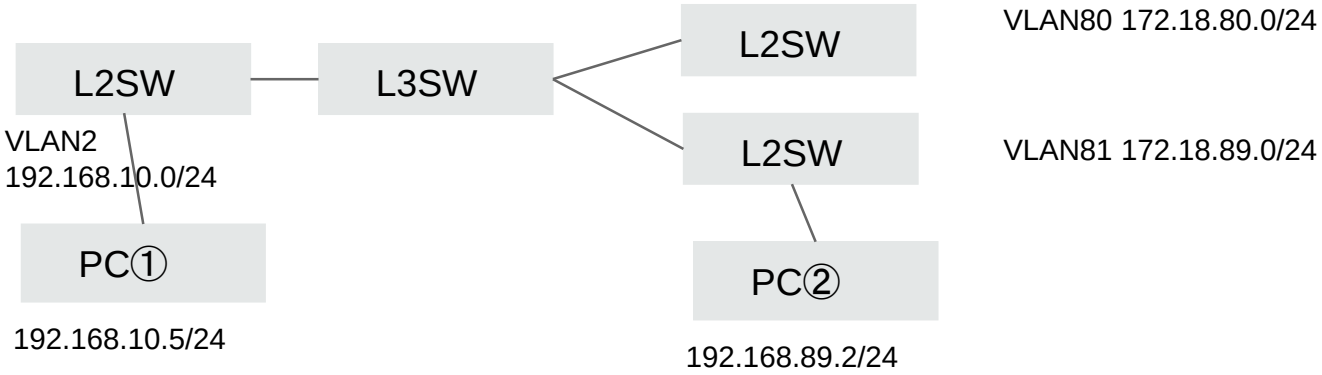
演習：PC（192.168.10.5)からPingで全VLAN-Interfaceに疎通できるか確認

演習：もう1台のPCに（VLAN81のネットワーク：172.18.89.2/24を設定)をInterfaceに接続

今やってる検証環境はこういうこと。L3SW1台でも検証できる



# ネットワーク/セキュリティエンジニア
# 実地研修




演習：PC1からPC2にPingを飛ばす　→疎通NG？

演習：PC1からVLAN2のデフォルトゲートウェイにPingを飛ばす　→L3SWまでは問題ないことを確認

演習：PC1からVLAN80のVLAN-InterfaceにPingを飛ばす　→VLAN80はOKなことを確認

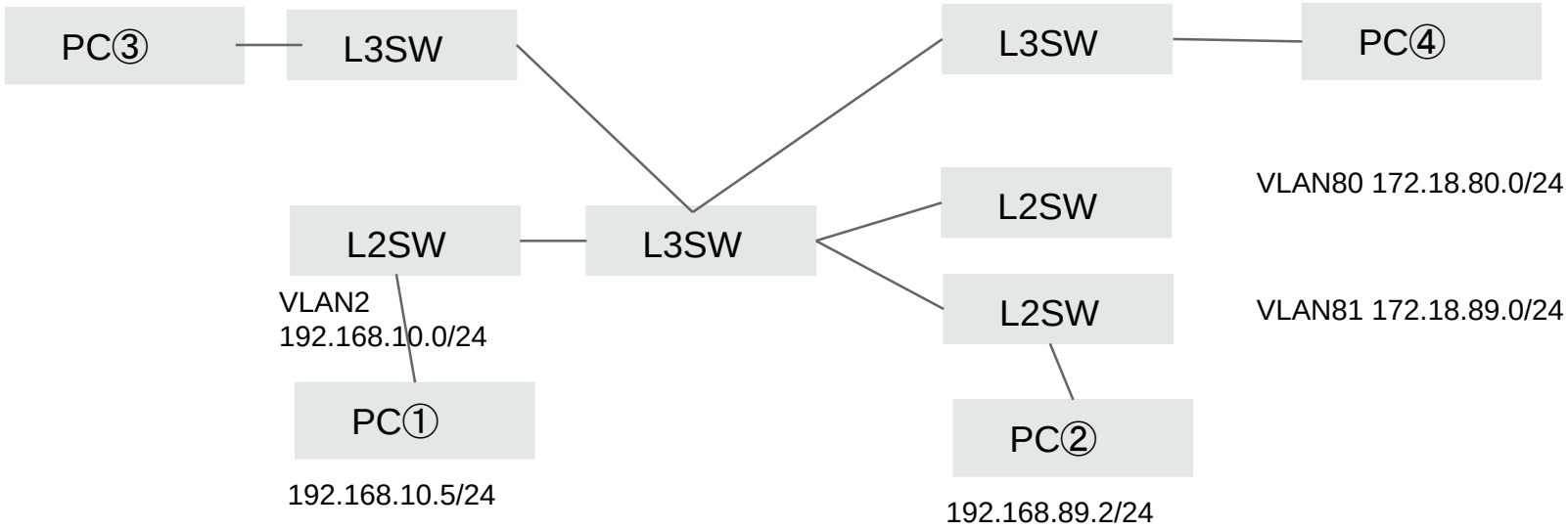
演習：PC1からVLAN81のVLAN-InterfaceにPingを飛ばす　→VLAN81はNGなことを確認　、なぜ？

答え：ACLを確認すること
ACLに192.168.89.2が許可されていないから

演習：PC1からPC2（172.18.89.1に変更して）にPingを飛ばす　→疎通OK

VLANの設定がOKであることが確認できた

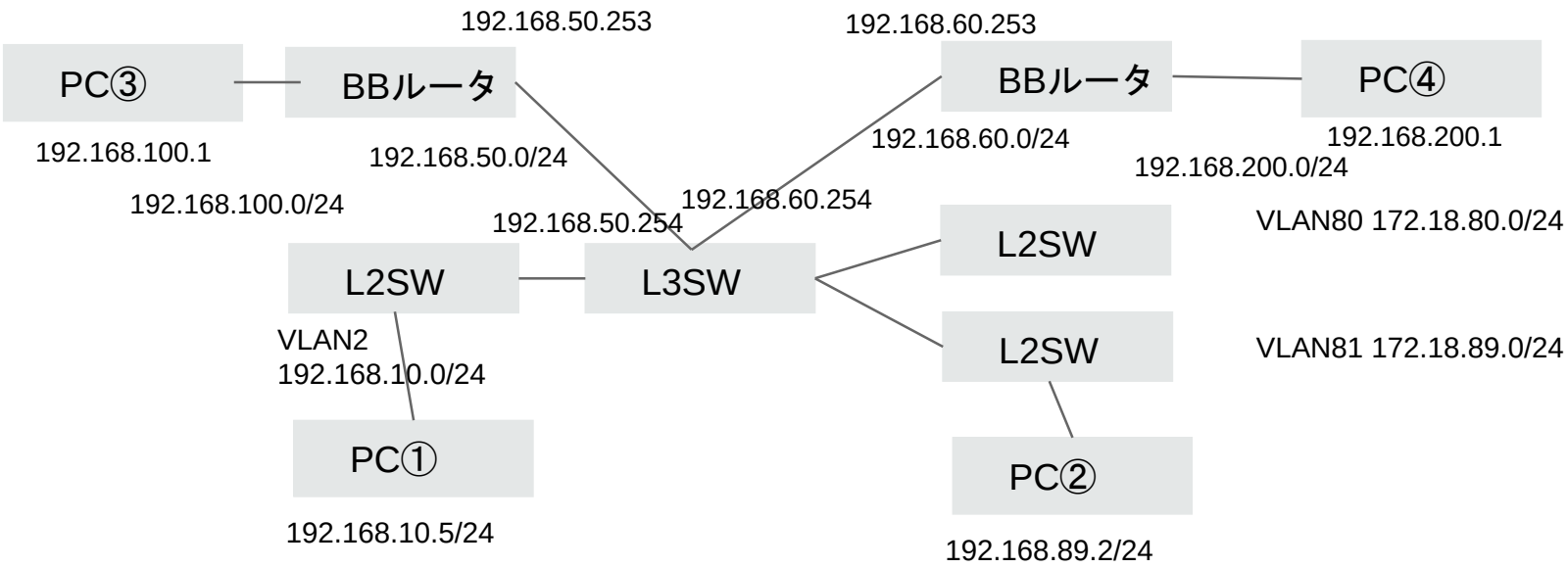
## （２）ルーティング（静的ルーティング、動的ルーティング）




PC①からPC③に行くためには？
L3SWでルート情報を設定してあげないといけない。
これまでルートはすべてデフォルトゲートウェイに任せていた。
しかし上図のようにルートが複数に分かれるとき、それぞれに応じたルーティング設定が必要

# ネットワーク/セキュリティエンジニア
# 実地研修

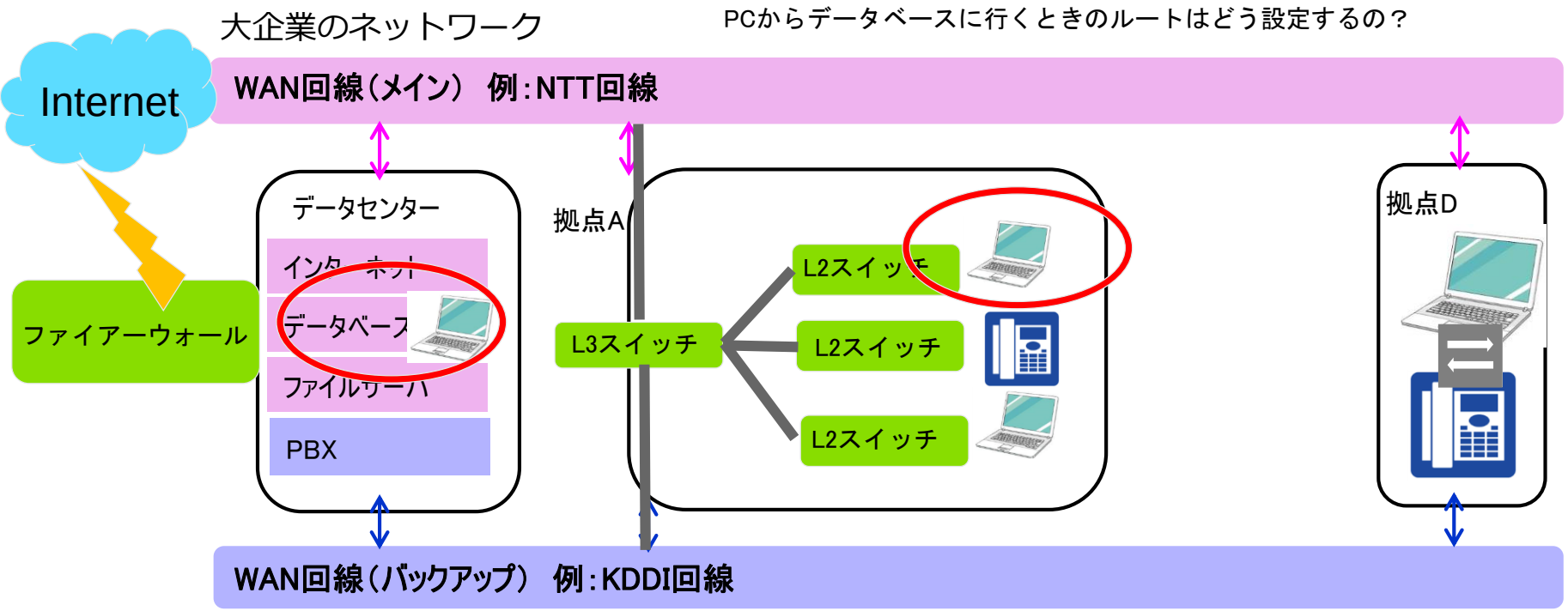
## （２）ルーティング（静的ルーティング、動的ルーティング）




L3SWで以下の設定
ip route 192.168.100.0 255.255.255.0 192.168.50.254 name Sapporo-route1
ip route 192.168.200.0 255.255.255.0 192.168.60.254 name Sapporo-route2

# ネットワーク/セキュリティエンジニア
# 実地研修

実際はこういうことをやっている



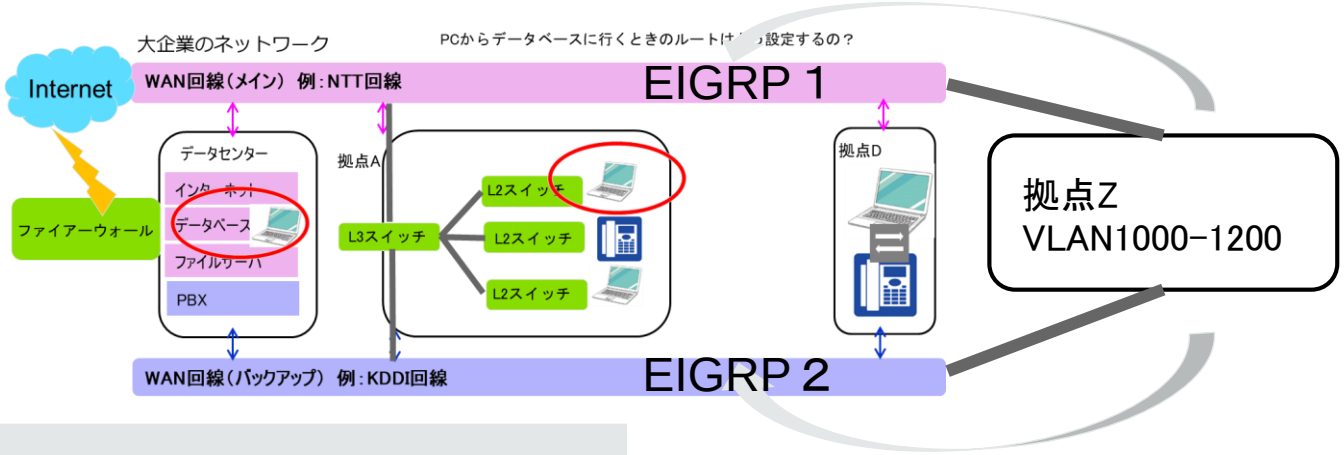
# ネットワーク/セキュリティエンジニア
# 実地研修

## 今までが静的ルーティング。
## では動的ルーティングとは？

大企業では拠点が100以上、ネットワーク（VLAN）が10000以上ということも珍しくない。
その場合、VLAN1つずつに人間がルーティングを書いていたらキリがない。
また拠点1つ追加したときに、10000分のルーティングを書くことは面倒。
そこで動的ルーティングが出てくる。

静的ルーティング　＝　スタティックルート
動的ルーティング　＝　ダイナミックルーティング　という言葉は重要。

動的ルーティングプロトコルにはいくつかあり、EIGRPがメリットも大きく主に使われる。




拠点ZのVLANそれぞれの情報が伝搬される

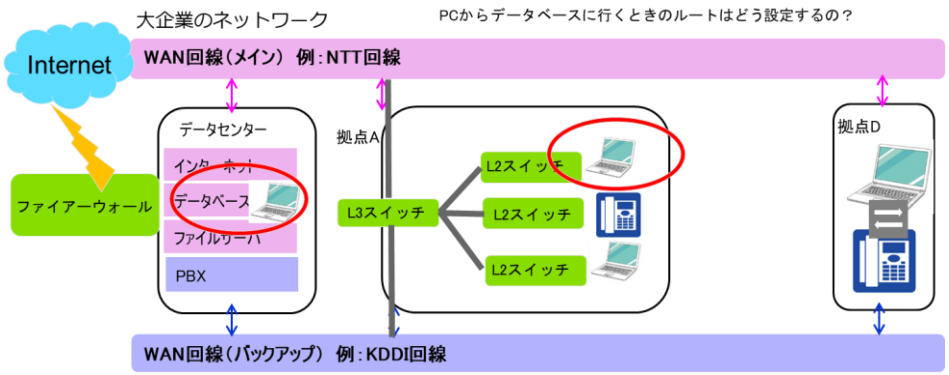
# ネットワーク/セキュリティエンジニア
# 実地研修

## どうやって冗長化している？

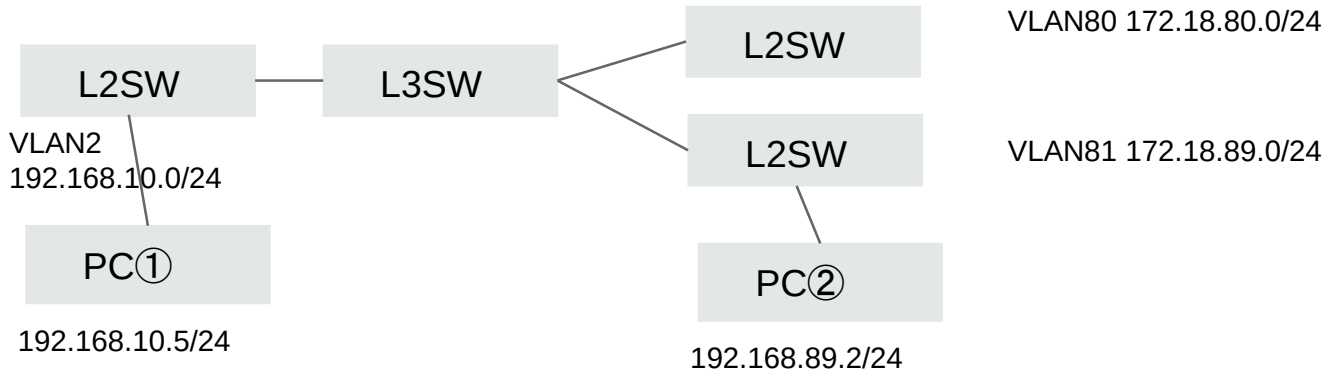
スタティックルートの場合、重みづけという方法があり、通常であればNTT回線を通ってデータベースに行く
もしNTT回線に障害が発生した場合は、KDDI回線を通ってデータベースに行くということを重みづけで設定できる

ダイナミックルートの場合も重みづけという方法で、通常であればNTT回線を通ってデータベースに行く（EIGRP１）
もしNTT回線に障害（EIGRP１）が発生した場合は、KDDI回線（EIGRP2）を通ってデータベースに行くということを
重みづけで設定できる

**この手法は難易度が高く、CCNP、ネットワークスペシャリストレベルの問題。設定できる人は少ない。設定を今覚える必要はないが、今では当たり前に使われているので概念は覚えること。**



## （３）ネットワークの分離



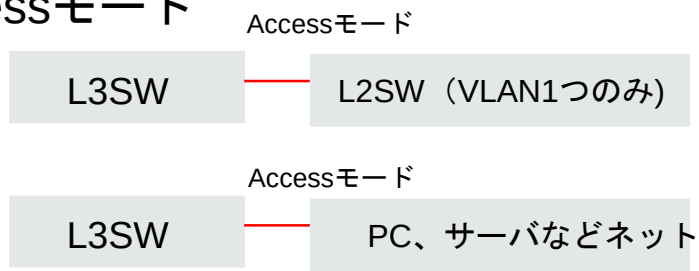

演習：VLAN2とVLAN80間は疎通できるように、VLAN2とVLAN81間は疎通できるように、
VLAN80とVLAN81は疎通できないように設定してみる。ACL名は何でもよい。
PCの設定もして実際にできるか試してみる。

# ネットワーク/セキュリティエンジニア
# 実地研修

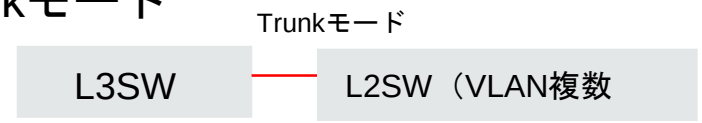
## （４） AccessモードとTrunk設定


L3SWでは、各InterfaceにAccessモードとTrunkモードのどちらかを設定しなければならない。

### Accessモード




### Trunkモード




L2SWの複数VLAN情報をL3SWに繋げる。

設定してみよう

```
interface fa 1/0/15
 description To Sapporo06-L2SW01 fa0/1
 switchport mode trunk
```

## 7　L2SWについて理解しよう

L2SWで気を付けなければならないのは、以下の点である。
・Trunkポート
・VLAN情報
・Spaning-Tree　（特に機器を追加する前には必ず確認すること）
・ループ構成になっていないか

絶対にこれだけは覚える。

L2SW追加時にSpaning-Treeの設定によっては
全ネットワークがダウンする！安易に追加しない！

## 8　L4以上ついて理解しよう

企業のNW構成では、L4以上の機器は外部とのセキュリティ、インターネットに出るための機器である。
L4以上を制御するため。
L4はアプリケーション、プロトコルレベルを指す。

例えば、HTTPは許可せず、SSLは許可する。
まずはプロトコルを覚えよう。


不要な通信はブロック！
必要な通信だけ外部と通信させる

# ネットワーク/セキュリティエンジニア
# 実地研修

## ９　セキュリティ概念を理解しよう

企業のNW構成で気を付けなければならないのは、ネットワークダウンとセキュリティ。
どっちが重要か？
セキュリティの方が重要である。

セキュリティ設定によっては情報漏洩で一発アウトもあり得る。（ベネッセなど）

セキュリティの概念を押さえておく。

**L3SW：**
**不要なルーティングは削除**
**通信許可、不許可をACLで制御**
**ファイアーウォール（最後の砦）：**
**不要な通信ポート（プロトコル）はブロック**
**通信ログは必ずON、数年の通信ログのバックアップも考える**
**外と中の通信許可、不許可設定を何度も見直す**
**外部の機関からも監視してもらう**
**外部攻撃検知機能、不要な通信検知機能、ウィルス検知機能をON**

# ネットワーク/セキュリティエンジニア
# 実地研修

## １０　セキュリティ対策

**ファイアーウォール（最後の砦）の設定が一番重要！**
**・分かりにくい機器は取り扱わない。**
**・セキュリティ検知機能は膨大なCPU、メモリが必要、**
**・PCがウィルス感染しても、FWでブロックして検知が求められる。**

ウィルス対策ソフトは1か月ほど遅れてパターンファイルが更新される。
国家間での攻撃では常に新しい未知のウィルスで標的型攻撃をしてくる。
そこでFW、IPS、IDSなどのゲートウェイ機器で検知する必要あり。
不正な通信、特に通信先が中国、ロシアで断続的な通信が発生していたり、
危険な通信先IPアドレスに行っていれば、不正と判断。

最近はポート番号を変える攻撃はなく、ほぼ全員が許可している
HTTP通信にターゲットを絞っているため、ポート制御は当然だが、
攻撃は防げない！L7レベルまでの機器が求められている。

# ネットワーク/セキュリティエンジニア
# 実地研修

**機器の選定基準（最新版）**

- **CPU、メモリ**
- **価格**
- **冗長化（障害に強い）**
- **設定がわかりやすい、見やすい**
- **IPS、IDS、ウィルス検知までの機能があるもの（別用意でもOK）**
- **（NEW）最新の危険先リストを世界中で同期できる機器**
  ※AIやイスラエルのスタートアップ企業が注目されている

外部からの攻撃には必ず情報を引き出すという作業がある。
つまり通信である。通信が発生する限り、セキュリティ機器、
FWで検知することが必要
アナログ的なやり方もセキュリティでは重要！